IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of	)	
	)	
Jean-Sebastien Coron et al.	)	Group Art Unit: 2131
	)	
Application No.: 09/913,884	)	Examiner: M. T. Henning
	)	
Filed: March 8, 2002	)	Confirmation No.: 5848
	)	
For: METHOD FOR COUNTERMEASURE IN AN ELECTRONIC COMPONENT USING A SECRET KEY ALGORITHM	)	

REPLY AFTER NOTICE OF ALLOWANCE

Mail Stop ISSUE FEE
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Applicant gratefully acknowledges the Notice of Allowance, mailed April 13, 2008. The Issue Fee is due in the subject application by November 13, 2008.

In an Office Action mailed November 29, 2005, the Examiner returned Applicant's Form 1449A provided with the Information Disclosure Statement ("IDS") dated August 17, 2001, and indicated that the listed French-language document FR 2672402A was not considered. It seems the Examiner did not consider the document because no English translation or explanation of its relevance was provided pursuant to 37 C.F.R. § 1.98(a)(3). However, as stated in M.P.E.P. § 609.3, no translation of the document is required.

M.P.E.P. § 609.3 states:

> The examiner will consider the documents cited in the international search report in a PCT national stage application when the Form PCT/DO/EO/903 indicates that both the international search report and the copies of the documents are present in the national stage file. In such a case, the examiner should consider the documents from the international search report and indicate by a statement in the first Office action that the information has been considered.

In the subject application, the Form PCT/DO/EO/903 (Notice of Acceptance of Application under 35 U.S.C. 371 and 37 CFR 1.495) indicates that the international search report and copies of the documents identified in the search report were received by the USPTO. A copy of the Form PCT/DO/EO/903 is attached hereto. For the Examiner's reference, a copy of FR 2672402A and a partial translation thereof are also attached.

Applicant respectfully submits that the IDS dated August 17, 2001, conforms with M.P.E.P. § 609. Therefore, it is requested that the Examiner consider FR 2672402A and return a signed and initialed copy of the Applicant's Form 1449A indicating that the reference has been considered.

Respectfully submitted,

BUCHANAN INGERSOLL & ROONEY PC

Date: September 11, 2008

By: /Steven Ashburn/
Steven L. Ashburn
Registration No. 56,636

Customer No. 21839

UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER OF PATENTS AND TRADEMARKS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

U.S. APPLICATION NUMBER NO.	FIRST NAMED APPLICANT	ATTY DOCKET NO.
09/913,884	Jean-Sebastien Coron	032326-161

INTERNATIONAL APPLICATION NO.	
PCT/FR00/00130	
I.A. FILING DATE	PRIORITY DATE
01/20/2000	02/17/1999

21839
BURNS DOANE SWECKER & MATHIS L L P
POST OFFICE BOX 1404
ALEXANDRIA, VA 22313-1404

CONFIRMATION NO. 5848

371 ACCEPTANCE LETTER

OC000000010057262

Date Mailed: 05/19/2003

NOTICE OF ACCEPTANCE OF APPLICATION UNDER 35 U.S.C 371 AND 37 CFR 1.495

The applicant is hereby advised that the United States Patent and Trademark Office in its capacity as a Designated / Elected Office (37 CFR 1.495), has determined that the above identified international application has met the requirements of 35 U.S.C. 371, and is ACCEPTED for national patentability examination in the United States Patent and Trademark Office.

The United States Application Number assigned to the application is shown above and the relevant dates are:

03/08/2002	03/08/2002
DATE OF RECEIPT OF 35 U.S.C. 371(c)(1), (c)(2) and (c)(4) REQUIREMENTS	DATE OF RECEIPT OF ALL 35 U.S.C. 371 REQUIREMENTS

A Filing Receipt (PTO-103X) will be issued for the present application in due course. **THE DATE APPEARING ON THE FILING RECEIPT AS THE " FILING DATE" IS THE DATE ON WHICH THE LAST OF THE 35 U.S.C. 371 REQUIREMENTS HAS BEEN RECEIVED IN THE OFFICE. THIS DATE IS SHOWN ABOVE.** *The filing date of the above identified application is the international filing date of the international application (Article 11(3) and 35 U.S.C. 363).* Once the Filing Receipt has been received, send all correspondence to the Group Art Unit designated thereon.

The following items have been received:

- Copy of the International Application filed on 08/17/2001
- English Translation of the IA filed on 03/08/2002
- Copy of the International Search Report filed on 08/17/2001
- Copy of IPE Report filed on 08/17/2001
- Preliminary Amendments filed on 08/17/2001
- Information Disclosure Statements filed on 08/17/2001
- Oath or Declaration filed on 01/16/2002
- Request for Immediate Examination filed on 08/17/2001
- Copy of references cited in ISR filed on 08/17/2001
- U.S. Basic National Fees filed on 08/17/2001
- Priority Documents filed on 08/17/2001

The following defects have been observed:

- Preliminary Amendments have not been entered because it does not reference those changes made to the claims in the IPER.

Applicant is reminded that any communications to the United States Patent and Trademark Office must be mailed to the address given in the heading and include the U.S. application no. shown above (37 CFR 1.5)

FRANCINE YOUNG
Telephone: (703) 305-3662

PART 3 - OFFICE COPY

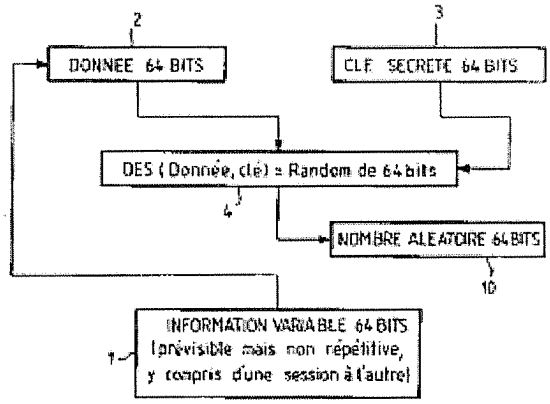
FORM PCT/DO/EO/903 (371 Acceptance Notice)

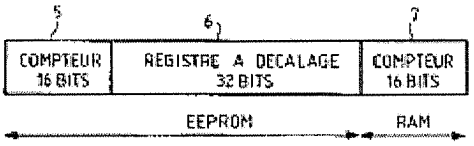
Process and device for generating unique pseudo-random numbers

Publication number: FR2672402
Publication date: 1992-08-07
Inventor: BALLOT-SCHMIT GERONIMI FRANCOI; GILLES VIRICEL
Applicant: GEMPLUS CARD INT (FR)
Classification:
- international: ***G06F7/58;* G06F7/58;** (IPC1-7): G06F7/58
- European: G06F7/58P; G06F7/58P3
Application number: FR19910001268 19910205
Priority number(s): FR19910001268 19910205

Abstract of **FR2672402**

The process consists in registering (1, 2) into a specified area of the non-volatile memory of a microcircuit memory card a specified and non-repetitive value item with each generating of a random number and in converting (3, 4) this item into an item having the form of a pseudo-random number by programming the processing unit by means of a standard information encrypting program of the DES type. Application: memory cards.





Single process and device for generating pseudo-random numbers

Description off **FR2672402** Translate this text

PROCESS AND DEVICE FOR THE GENERATION
SINGLE PSEUDO-RANDOM NUMBERS
The present invention relates to a process and a device for the generation of single pseudo-random numbers.

It applies in particular to the realization of charts with microcircuits said to chips usable in any system where the access to information or services is severely controlled. They are in particular the systems distributors of fiduciary currency, of the field of the systems of television to toll; systems for the distribution of gasoline or domestic oil; systems for the access to data banks etc...

In the smart cards with microprocessor which are used in the preceding fields, the access to information or services is severely controlled. One uses for that of the passwords. These passwords are more and more often transmitted by cryptant them by a pseudo-random code provided by a generator to programmed or possibly cabled structure. In the smart cards containing microprocessors, there exists in the state of the art only material generators (based on physical phenomena) or software generators based on properties mathematical and already used in the traditional computing world. These two principles cannot guarantee the unicity of the generated numbers what presents a major disadvantage of safety as regards modern cryptography.

If this solution has the advantage of not informing the defrauders about the passwords used, it indeed leaves the possibility to the latter of recopying the transmitted encrypted passwords which, from their defect of unicity, can always be re-used to give the access to information or services for which the chart is dedicated. Indeed, it is then enough to renew the experiment so as to find a value already used and thus to defraud the system.

In addition, the production of random number single runs up against the technological possibilities of rewriting in nonvolatile memories. Each cell cannot indeed be rewritten more than 10.000 times. The goal de11 invention is to mitigate the above mentioned disadvantages.

For this purpose, the invention has as an aim a process for the generation of single pseudo-random numbers in a smart card with microcircuits comprising at least a rewriteable nonvolatile memory (EEPROM) coupled to a body of data processing, characterized in that it consists
- to register in a given zone of the memory, information of given and nonrepetitive value to each generation of a random number and,
- to convert this information into information having the form of a pseudo-random number while making him undergo in the body of data processing a programme of encoding of the type DES.

It also has as an aim a device for implemented of the process.

The invention has moreover as an main advantage allowing, by using a meter which comprises a shift register, to compared obtain a very high number of pullings of random numbers to the number of cycles of obliteration/writing authorized in the nonvolatile memory usually equipping the smart cards. Thus, in spite of an erase count/writing limited to 10.000 by current technology of the nonvolatile, still known memories under designation
EEPROM, it is possible, thanks to the invention, to generate in worst case 320.000 values different and in the best from the cases 21 billion, by using a memory capacity very reduced EEPROM of 64 bits.

Other characteristics and advantages of the invention will appear hereafter using the description which follows made compared to the annexed drawings which represent
Figure 1: a procedure of the process according to the invention put in the shape of a flow chart.

Figure 2: a format of an information word usable for the implementation of the process according to the invention represented by the flow chart of figure 1.

In its most general definition, a smart card for the application of the process according to the invention comprises, in a way known and not represented, a device of memorizing and a processor formed normally by a microprocessor or any equivalent device, couplésl' one with the other by a data bus and addresses. This bus also ensures the connection of the microcircuit of the chart thus formed, with devices of writing and reading outsides to the chart. The device of memorizing generally comprises a nonvolatile memory, of type EPROM or
EEPROM, in which are recorded microprograms necessary to the operation of the processor and normally a volatile random access memory of type RAM.Cette last is useful for temporary memorizing of the data and the specific instructions of the application in progress with the smart card. In the nonvolatile memory are arranged, for example, on the one hand the secret code identifying the holder of the chart, with possibly a programme of coding for obtaining a signature calculated on the basis of of the secret code and, on the other hand, instructions of the program of use itself.

The process according to the invention whose stages 1 to 4 are represented schematically on the flow chart of figure 1 consists in, each time a random number 10 is to be produced, calculating according to stages 1 and 2, starting from a data 1 of given information (length NR = 64 bits for example), a new data 2 of the same length NR, but whose value could not again any more be generated at the time of a later request of new data 2. Once transformed, data 2 is at stage 4 associated with a secret key 3 comprising the same number of bits, by a calculation algorithm commonly known under the Anglo-Saxon abbreviation OF "Data Encryption Standard" and of which a description can be found in the booklets of standards FIPS of "Federal Information Processing Standards" of
States-Unisd 'America.

The superiority of the algorithm of association OF on the other algorithms of association is that it makes it possible to obtain for each constant secret key 3 length of NR bits, the 2N possible combinations of the result by always guaranteeing the nonforeseeable character of the random number 10, i.e., to always obtain different random numbers 10.

This is obtained starting from the 2N possible combinations of the input datum. But the fact that the key has a length of NR bits has nothing to do with the fact that there is 2N different combinations on the result. This is related to the fact that the input datum with a length of NR bits. For example, the characteristics of indicate that for a constant key secret, the 264 possible combinations of the data sweep the 264 possible combinations of the result what guarantees, in addition to the nonforeseeable nature of the random number (related to the performances of), the property always to obtain different random numbers. In the invention, one will have thus a constant secret key 3.

To obtain this result, each data 2 of variable information is structured way which is represented on figure 2. Its format comprises three zones, a first zone 5 of capacity equalizes for example with 16 bits represents the states taken by a first meter, a second zone 6 of capacity equalizes for example with 32 bits represents the states of a shift register and, a third zone 7 of capacity equalizes for example with 16 bits represents the states of a second meter. The first and second zones 5 and 6 are then located in a nonvolatile memory of the chart whereas zone 7 is located in random access memory. According to the invention, the contents of the three zones are regarded as equivalent with that which would be given by a meter of NR bits which would be incremented with each request for calculation. This information is thus foreseeable but is always different from the preceding values. Storage in memory EEPROM of the data of zones 5 and 6 makes it possible to preserve the values of their contents when the supply voltage of the chart is removed.

This solution makes it possible to obtain a maximum number of random numbers much higher than the 10.000 authorized by technology EEPROM.

The zone 6, which is organized in shift register, makes it possible to obtain a maximum number of random number. For that, with each new calculation or session, a bit of value 1 is in charge with the last position of the weakest weight of the register which is still to 0. When 32 requests for calculation, corresponding to the setting with 1 of the 32 bits of register 6 with shift, are carried out, following calculation gives to zero the shift register represented by zone 6. When 32 calculations were carried out, the shift register is with value FFFFFFFFH although each bit was written only once. One thus obtains 32 different values by consuming only one writing for each cell. With each obliteration of this register of 32 bits, the meter of 16 bits of zone 5 in EEPROM being incremented what ultimately makes it possible to obtain, 32 X 10000 = 320000 unforeseeable and nonrepetitive values for data 2 (without none the bits handled in
EEPROM unobtrusive/is not written more than 10000 times). To obtain a greater quantity of values (out worse case), it is enough to associate with this variable of 48 bits in EEPROM, a meter 7 of 16 bits in RAM

which will be incremented with each calculation in the same session.

Zone 7 located in memory RAM thus makes it possible to increase the number of the preceding values while increasing, in a way similar to the meter materialized by zone 5, the contents of the meter materialized by zone 7 with each new calculation in the same session.

If it arrives in the same session that this meter overflows, i.e. its contents exceed 65536 values here, one can modify the contents of the shift register materialized by zone 6 of memory EEPROM as if a new session started. In this case, one puts at 1 another bits of this register 6.

On the whole, this provision allows while concaténant, i.e. by juxtaposing the 48 bits in EEPROM with the 16 bits located in memory RAM, to obtain 320.000 X 65536 is approximately 21 billion unforeseeable and nonrepetitive values by the implementation of a calculation of random numbers by using the algorithm AS OF previously quoted.

By safety, one associates with meter 5 of 16 bits in EEPROM an meter-image in EEPROM. This meter-image always contains the same value that the genuine meter and is used if the value of the meter is destroyed (pulling up of the chart when the meter has just been unobtrusive to modify the value of it). It is not necessary to envisage the same thing for the shift register because this one is unobtrusive only for its restoring.

The structure of the meter thus used (including/understanding a shift register) makes it possible to obtain a number of pullings very high compared to the number of cycles of obliteration/writing (updated) authorized in the nonvolatile memory. Thus, in spite of a nombred' obliteration/writing limited to 10000 by technology EEPROM, one manages to generate in worst case 320.000 values different and in the best from the cases 21 billion.

Single process and device for generating pseudo-random numbers

Claims off **FR2672402** Translate this text

CLAIMS

1. Proceeded for the generation of single pseudo-random numbers in a smart card to microcircuits comprising at least a rewriteable nonvolatile memory (EEPROM) coupled to a body of data processing characterized in that it consists,
- to register (1,2) in a given zone of the memory, information of given and nonrepetitive value to each generation of a random number and,
- to convert (3,4) this information into information having the form of a pseudo-random number while making him undergo in the body of data processing a programme of encoding of the type DES.

2. Proceeded according to claim 1, characterized in that the information of given and nonrepetitive value is registered in a memory EEPROM of the chart.

3. Proceeded according to claim 2, characterized in that the information of given and nonrepetitive value is structured according to at least two zones, a first zone (6) to write in a systematic way at least a new bit each time a pseudo-random number is generated by the chart, and a second zone (5) of counting to add up the number of times where the first zone was completely written.

4. Proceeded according to claim 3, characterized in that it consists in structuring information of given and nonrepetitive value by adding to him a third zone (7) of counting to add up the number of times where, in the same session, a pseudo-random number was generated.

5. Proceeded according to claim 4, characterized in that the first and second zones (6, 5) are memorized in a nonvolatile memory of the chart and in what the third zone (7) is memorized in a volatile memory of the chart.

6. Process according to claim 3, characterized in that one holds a third zone to be used as image of the result of the counting added up in the second zone.

7. Device for the implementation of the process according to any of claims 1 to 6, characterized in that it is formed by a chart with microcircuit comprising a treatment unit coupled to a nonvolatile memory and with a volatile memory.

---

(19) RÉPUBLIQUE FRANÇAISE

INSTITUT NATIONAL
DE LA PROPRIÉTÉ INDUSTRIELLE

PARIS

(11) N° de publication : **2 672 402**
(à n'utiliser que pour les commandes de reproduction)

(21) N° d'enregistrement national : **91 01268**

(51) Int Cl[5] : G 06 F 7/58

(12) DEMANDE DE BREVET D'INVENTION A1

(22) **Date de dépôt** : 05.02.91.

(30) **Priorité** :

(43) **Date de la mise à disposition du public de la demande :** 07.08.92 Bulletin 92/32.

(56) **Liste des documents cités dans le rapport de recherche :** *Se reporter à la fin du présent fascicule.*

(60) **Références à d'autres documents nationaux apparentés :**

(71) **Demandeur(s) :** *Société Anonyme dite GEMPLUS CARD INTERNATIONAL* — FR.

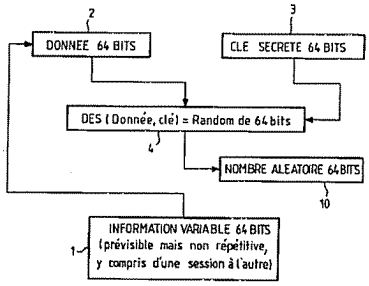
(72) **Inventeur(s) :** Geronimi François Cabinet Ballot-Schmit et Viricel Gilles.

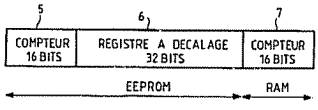
(73) **Titulaire(s) :**

(74) **Mandataire :** Cabinet Ballot-Schmit.

(54) Procédé et dispositif pour la génération de nombres pseudo-aléatoires uniques.

(57) Le procédé consiste à inscrire (1, 2) dans une zone déterminée de la mémoire non volatile d'une carte à mémoire à microcircuit une information de valeur déterminée et non répétitive à chaque génération d'un nombre aléatoire et à convertir (3, 4) cette information en une information ayant la forme d'un nombre pseudo-aléatoire en programmant l'unité de traitement au moyen d'un programme de cryptage de l'information standard, type DES.
Applications: cartes à mémoire.





FR 2 672 402 - A1

PROCEDE ET DISPOSITIF POUR LA GENERATION DE NOMBRES PSEUDO-ALEATOIRES UNIQUES

La présente invention concerne un procédé et un dispositif pour la génération de nombres pseudo-aléatoires uniques.

Elle s'applique notamment à la réalisation de cartes à microcircuits dites à puces utilisables dans tout système où l'accès à des informations ou à des services est sévèrement contrôlé. Il s'agit notamment des systèmes distributeurs de monnaie fiduciaire, du domaine des systèmes de télévision à péage ; des systèmes pour la distribution d'essence ou de fuel domestique ; des systèmes pour l'accès aux banques de données etc...

Dans les cartes à mémoire à microprocesseur qui sont utilisées dans les domaines précédents, l'accès à des informations ou à des services est sévèrement contrôlé. On utilise pour cela des mots de passe. Ces mots de passe sont de plus en plus souvent transmis en les cryptant par un code pseudo-aléatoire fourni par un générateur à structure programmée ou éventuellement câblée. Dans les cartes à mémoire à base de microprocesseurs, il n'existe dans l'état de la technique que des générateurs matériels (basé sur des phénomènes physiques) ou des générateurs logiciels basé sur des propriétés mathématiques et déjà utilisés dans le monde informatique traditionnel. Ces deux principes ne peuvent pas garantir l'unicité des nombres générés ce qui présente un inconvénient majeur de sécurité en matière de cryptographie moderne.

Si cette solution présente l'avantage de ne pas renseigner les fraudeurs sur les mots de passe

utilisés, elle laisse en effet la possibilité à ces derniers de recopier les mots de passe cryptés transmis qui, de par leur défaut d'unicité, peuvent toujours être réutilisés pour donner l'accès aux informations ou services pour lesquels la carte est dédiée. En effet, il suffit alors de renouveler l'expérience de manière à retrouver une valeur déjà utilisée et ainsi frauder le système.

Par ailleurs, la production de nombre aléatoire unique se heurte aux possibilités technologiques de réécriture dans des mémoires non volatiles. Chaque cellule ne peut en effet être réécrite plus de 10.000 fois. Le but de l'invention est de pallier les inconvénients précités.

A cet effet, l'invention a pour objet un procédé pour la génération de nombres pseudo-aléatoires uniques dans une carte à mémoire à microcircuits comportant au moins une mémoire non volatile réinscriptible (EEPROM) couplée à un organe de traitement de données, caractérisé en ce qu'il consiste

- à inscrire dans une zone déterminée de la mémoire, une information de valeur déterminée et non répétitive à chaque génération d'un nombre aléatoire et,
- à convertir cette information en une information ayant la forme d'un nombre pseudo-aléatoire en lui faisant subir dans l'organe de traitement de données un programme de cryptage de type DES.

Elle a également pour objet un dispositif pour la mis en oeuvre du procédé.

L'invention a en outre pour principal avantage de permettre, en utilisant un compteur qui comporte un registre à décalage, d'obtenir un nombre de tirages très élevé de nombres aléatoires comparativement au nombre de cycles d'effacement/écriture autorisés dans la mémoire

non volatile équipant habituellement les cartes à mémoire. Ainsi, malgré un nombre d'effacement/écriture limité à 10.000 par la technologie actuelle des mémoires non volatiles, encore connues sous la désignation EEPROM, il est possible, grâce à l'invention, de générer dans le pire des cas 320.000 valeurs différentes et dans le meilleur des cas 21 milliards, en utilisant un espace mémoire EEPROM très réduit de 64 bits.

D'autres caractéristiques et avantages de l'invention apparaîtront ci-après à l'aide de la description qui suit faite en regard des dessins annexés qui représentent :

Figure 1 : un mode d'exécution du procédé selon l'invention mis sous la forme d'un organigramme.

Figure 2 : un format d'un mot d'information utilisable pour la mise en oeuvre du procédé selon l'invention représenté par l'organigramme de la figure 1.

Dans sa définition la plus générale, une carte à mémoire pour l'application du procédé selon l'invention comporte, de façon connue et non représentée, un dispositif de mémorisation et un organe de traitement formé normalement par un microprocesseur ou tout dispositif équivalent, couplés l'un à l'autre par un bus de données et d'adresses. Ce bus assure également la liaison du microcircuit de la carte ainsi formée, avec des dispositifs d'écriture et de lecture extérieurs à la carte. Le dispositif de mémorisation comporte généralement une mémoire non volatile, de type EPROM ou EEPROM, dans laquelle sont enregistrés des microprogrammes nécessaires au fonctionnement de l'organe de traitement et normalement une mémoire vive volatile de type RAM. Cette dernière sert pour la mémorisation temporaire des données et des instructions

spécifiques de l'application en cours avec la carte à mémoire. Dans la mémoire non volatile sont rangés, par exemple, d'une part le code secret identifiant le titulaire de la carte, avec éventuellement un programme de chiffrement pour l'obtention d'une signature calculée sur la base du code secret et, d'autre part, des instructions du programme d'utilisation lui-même.

Le procédé selon l'invention dont les étapes 1 à 4 sont représentées schématiquement sur l'organigramme de la figure 1 consiste, chaque fois qu'un nombre aléatoire 10 est à produire, à calculer suivant les étapes 1 et 2, à partir d'une donnée 1 d'information déterminée (de longueur N = 64 bits par exemple), une nouvelle donnée 2 de même longueur N, mais dont la valeur ne pourra plus à nouveau être générée lors d'une requête ultérieure de nouvelle donnée 2. Une fois transformée, la donnée 2 est à l'étape 4 associée à une clef secrète 3 comportant un même nombre de bits, par un algorithme de calcul communément connu sous l'abréviation anglo-saxonne DES de "Data Encryption Standard" et dont une description peut être trouvée dans les brochures des normes FIPS des "Federal Information Processing Standards" des Etats-Unis d'Amérique.

La supériorité de l'algorithme d'association DES sur les autres algorithmes d'association est qu'il permet d'obtenir pour chaque clef secrète constante 3 de longueur de N bits, les 2^N combinaisons possibles du résultat en garantissant toujours le caractère non prévisible du nombre aléatoire 10, c'est-à-dire, d'obtenir toujours des nombres aléatoires différents 10. Ceci est obtenu à partir des 2^N combinaisons possibles de la donnée en entrée. Mais le fait que la clé ait une longueur de N bits n'a rien à voir avec le fait qu'il y ait 2^N combinaisons différentes sur le résultat. Ceci

est lié au fait que la donnée en entrée à une longueur de N bits. Par exemple, les caractéristiques de DES indiquent que pour une clef secrète constante, les 2^{64} combinaisons possibles de la donnée balaient les 2^{64} combinaisons possibles du résultat ce qui garantit, en plus du caractère non prévisible du nombre aléatoire (lié aux performances de DES), la propriété de toujours obtenir des nombres aléatoires différents. Dans l'invention, on disposera ainsi d'une clef secrète constante 3.

Pour obtenir ce résultat, chaque donnée 2 d'information variable est structurée de la façon qui est représentée à la figure 2. Son format comporte trois zones, une première zone 5 de capacité égale par exemple à 16 bits représente les états pris par un premier compteur, une deuxième zone 6 de capacité égale par exemple à 32 bits représente les états d'un registre à décalage et, une troisième zone 7 de capacité égale par exemple à 16 bits représente les états d'un deuxième compteur. Les première et deuxième zones 5 et 6 sont alors situées dans une mémoire non volatile de la carte alors que la zone 7 est située en mémoire vive. Selon l'invention, le contenu des trois zones est considéré comme équivalent à celui qui serait donné par un compteur de N bits qui serait incrémenté à chaque demande de calcul. Cette information est donc prévisible mais est toujours différente des valeurs précédentes. Le stockage en mémoire EEPROM des données des zones 5 et 6 permet de conserver les valeurs de leur contenu lorsque la tension d'alimentation de la carte est supprimée. Cette solution permet d'obtenir un nombre maximum de nombres aléatoires très supérieur aux 10.000 autorisés par la technologie EEPROM.

La zone 6, qui est organisée en registre à

décalage, permet d'obtenir un nombre maximum de nombre aléatoires. Pour cela, à chaque nouveau calcul ou session, un bit de valeur 1 est chargé à la dernière position de poids le plus faible du registre qui est encore à 0. Lorsque 32 demandes de calcul, correspondant à la mise à 1 des 32 bits du registre 6 à décalage, sont effectuées, le calcul suivant remet à zéro le registre à décalage représenté par la zone 6. Lorsque les 32 calculs ont été réalisés, le registre à décalage est à la valeur FFFFFFFFH bien que chaque bit n'ait été écrit qu'une seule fois. On obtient ainsi 32 valeurs différentes en ne consommant qu'une seule écriture pour chaque cellule. A chaque effacement de ce registre de 32 bits, le compteur de 16 bits de la zone 5 en EEPROM sera incrémenté ce qui en définitive permet d'obtenir, 32 X 10000 = 320000 valeurs imprévisibles et non répétitives pour la donnée 2 (sans qu'aucun des bits manipulés en EEPROM ne soit effacé/écrit plus de 10000 fois). Pour obtenir une plus grande quantité de valeurs (hors pire cas), il suffit d'adjoindre à cette variable de 48 bits en EEPROM, un compteur 7 de 16 bits en RAM qui sera incrémenté à chaque calcul dans une même session.

La zone 7 située en mémoire RAM permet donc d'augmenter le nombre des valeurs précédentes en augmentant, de manière similaire au compteur matérialisé par la zone 5, le contenu du compteur matérialisé par la zone 7 à chaque nouveau calcul dans une même session. S'il arrive dans une même session que ce compteur déborde, c'est-à-dire que son contenu dépasse ici 65536 valeurs, on peut modifier le contenu du registre à décalage matérialisé par la zone 6 de la mémoire EEPROM comme si une nouvelle session commençait. Dans ce cas, on met à 1 un autre des bits de ce registre 6.

Au total, cette disposition permet en concaténant,

c'est-à-dire en juxtaposant les 48 bits en EEPROM aux 16 bits situés en mémoire RAM, d'obtenir 320.000 X 65536 soit environ 21 milliards de valeurs imprévisibles et non répétitives par la mise en oeuvre d'un calcul de nombres aléatoires en utilisant l'algorithme DES précédemment cité.

Par sécurité, on associe au compteur 5 de 16 bits en EEPROM un compteur-image en EEPROM. Ce compteur-image contient toujours la même valeur que le véritable compteur et est utilisé dans le cas où la valeur du compteur est détruite (arrachage de la carte lorsque le compteur vient d'être effacé pour en modifier la valeur). Il n'est pas nécessaire de prévoir la même chose pour le registre à décalage car celui-ci n'est effacé que pour sa remise à zéro.

La structure du compteur ainsi utilisée (comprenant un registre à décalage) permet d'obtenir un nombre de tirages très élevé comparativement au nombre de cycles d'effacement/écriture (mise à jour) autorisé dans la mémoire non volatile. Ainsi, malgré un nombre d'effacement/écriture limité à 10000 par la technologie EEPROM, on arrive à générer dans le pire des cas 320.000 valeurs différentes et dans le meilleur des cas 21 milliards.

REVENDICATIONS

1. Procédé pour la génération de nombres pseudo-aléatoires uniques dans une carte à mémoire à microcircuits comportant au moins une mémoire non volatile réinscriptible (EEPROM) couplée à un organe de traitement de données caractérisé en ce qu'il consiste,

- à inscrire (1,2) dans une zone déterminée de la mémoire, une information de valeur déterminée et non répétitive à chaque génération d'un nombre aléatoire et,

- à convertir (3,4) cette information en une information ayant la forme d'un nombre pseudo-aléatoire en lui faisant subir dans l'organe de traitement de données un programme de cryptage de type DES.

2. Procédé selon la revendication 1, caractérisé en ce que l'information de valeur déterminée et non répétitive est inscrite dans une mémoire EEPROM de la carte.

3. Procédé selon la revendication 2, caractérisé en ce que l'information de valeur déterminée et non répétitive est structurée suivant au moins deux zones, une première zone (6) pour écrire de façon systématique au moins un nouveau bit chaque fois qu'un nombre pseudo-aléatoire est généré par la carte, et une deuxième zone (5) de comptage pour totaliser le nombre de fois où la première zone a été totalement écrite.

4. Procédé selon la revendication 3, caractérisé en ce qu'il consiste à structurer l'information de valeur déterminée et non répétitive en lui rajoutant une troisième zone (7) de comptage pour totaliser le nombre de fois où, dans une même session, un nombre pseudo-aléatoire a été généré.

5. Procédé selon la revendication 4, caractérisé en ce que les première et deuxième zones (6, 5) sont mémorisées dans une mémoire non volatile de la carte et en ce que la troisième zone (7) est mémorisée dans une mémoire volatile de la carte.

6. Procédé selon la revendication 3, caractérisé en ce qu'on réserve une troisième zone pour servir d'image du résultat du comptage totalisé dans la deuxième zone.

7. Dispositif pour la mise en oeuvre du procédé selon l'une quelconque des revendications 1 à 6, caractérisé en ce qu'il est formé par une carte à microcircuit comportant une unité de traitement couplée à une mémoire non volatile et à une mémoire volatile.

FIG_1

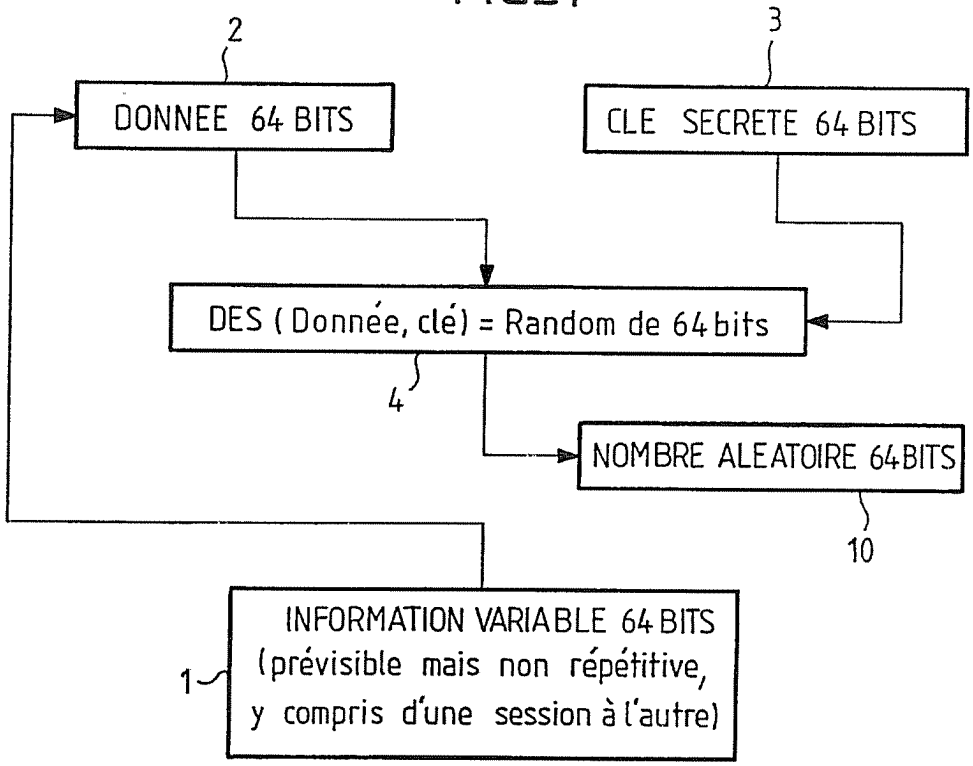
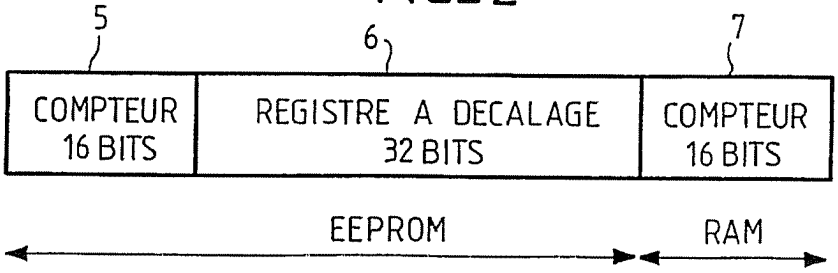

2
3
DONNEE 64 BITS
CLE SECRETE 64 BITS
DES (Donnée, clé) = Random de 64 bits
4
NOMBRE ALEATOIRE 64 BITS
10
INFORMATION VARIABLE 64 BITS
(prévisible mais non répétitive,
y compris d'une session à l'autre)
1

FIG_2


5
6
7
COMPTEUR
16 BITS
REGISTRE A DECALAGE
32 BITS
COMPTEUR
16 BITS
EEPROM
RAM

REPUBLIQUE FRANÇAISE

2672402

INSTITUT NATIONAL
de la
PROPRIETE INDUSTRIELLE

RAPPORT DE RECHERCHE

établi sur la base des dernières revendications déposées avant le commencement de la recherche

N° d'enregistrement national

FR 9101268
FA 454010

DOCUMENTS CONSIDERES COMME PERTINENTS

Catégorie	Citation du document avec indication, en cas de besoin, des parties pertinentes	Revendications concernées de la demande examinée
Y	EP-A-0386677 (SIEMENS) * le document en entier * ---	1, 2, 7
Y	EP-A-0284133 (TRT) * le document en entier * ---	1, 2, 7
A	US-A-4802217 (MICHENER) * le document en entier * -----	1

DOMAINES TECHNIQUES RECHERCHES (Int. Cl.5)

G06F

Date d'achèvement de la recherche	Examinateur
05 SEPTEMBRE 1991	DURAND, J

CATEGORIE DES DOCUMENTS CITES

X : particulièrement pertinent à lui seul
Y : particulièrement pertinent en combinaison avec un autre document de la même catégorie
A : pertinent à l'encontre d'au moins une revendication ou arrière-plan technologique général
O : divulgation non-écrite
P : document intercalaire

T : théorie ou principe à la base de l'invention
E : document de brevet bénéficiant d'une date antérieure à la date de dépôt et qui n'a été publié qu'à cette date de dépôt ou qu'à une date postérieure.
D : cité dans la demande
L : cité pour d'autres raisons

& : membre de la même famille, document correspondant

EPO FORM 1503 03.82 (P0413)